

BİL 470
KRİPTOGRAFI VE AĞ GÜVENLİĞİ
ÖDEV 1

ANALİZ :

- Özet fonksiyonlar arasındaki farkları ve güvenlik değerini tartışın.

MD5 - SHA Karşılaştırması [1]

- MD5'in çıktısı 128 bit iken, SHA'nın çıktısı 160 bittir. Yani MD5'te 4 adet 32 bitlik değişken kullanılırken, SHA'da 5 adet 32 bitlik değişken kullanılır.
- Her ikisinde 512 bitlik bloklar üzerinde işlem yaparlar.
- SHA'da ekleme (padding) işlemi, MD5'teki ile aynı şekilde yapılır.
- SHA'da da her 512 bitlik blok için 4 adımda işlemler yapılır, fakat bir farkla: MD5'de her adımda önceden tanımlı işlevlerin kullanımı 16 kez tekrarlanırken, bu sayı SHA'da 20 kezdir.
- SHA girdi olarak maksimum 2^{64-1} uzunluğunda veriyi kabul eder. Bunu yanında MD5 için böyle bir kısıtlama yoktur.
- SHA ürettiği 160 bitlik sonuç ile brute-force (bütün olası sonuçların denenmesi ile gerçekleştirilir) ataklara karşı daha dayanıklıdır.

❖ Genel olarak SHA, MD5 ten daha güvenlidir.

Diğer Hash Fonksiyonlar

MD5 ve SHA'nın yanında daha birçok MD algoritması tasarlanmıştır. Bunlardan bazıları: MD2, MD4, Haval, Ripe-MD, Snefru, N-Hash'dır.

- Veri şifreleme için özet fonksiyonların güvenlik seviyesini tartışın.

Özetleme fonksiyonları, mesaj şifrelemede değil, ya veri güvenliğinde verinin farklı olup olmadığını kontrol etmeye yarar ya da verileri sınıflandırmak için kullanılır. Çünkü çok güvenilir değildir.

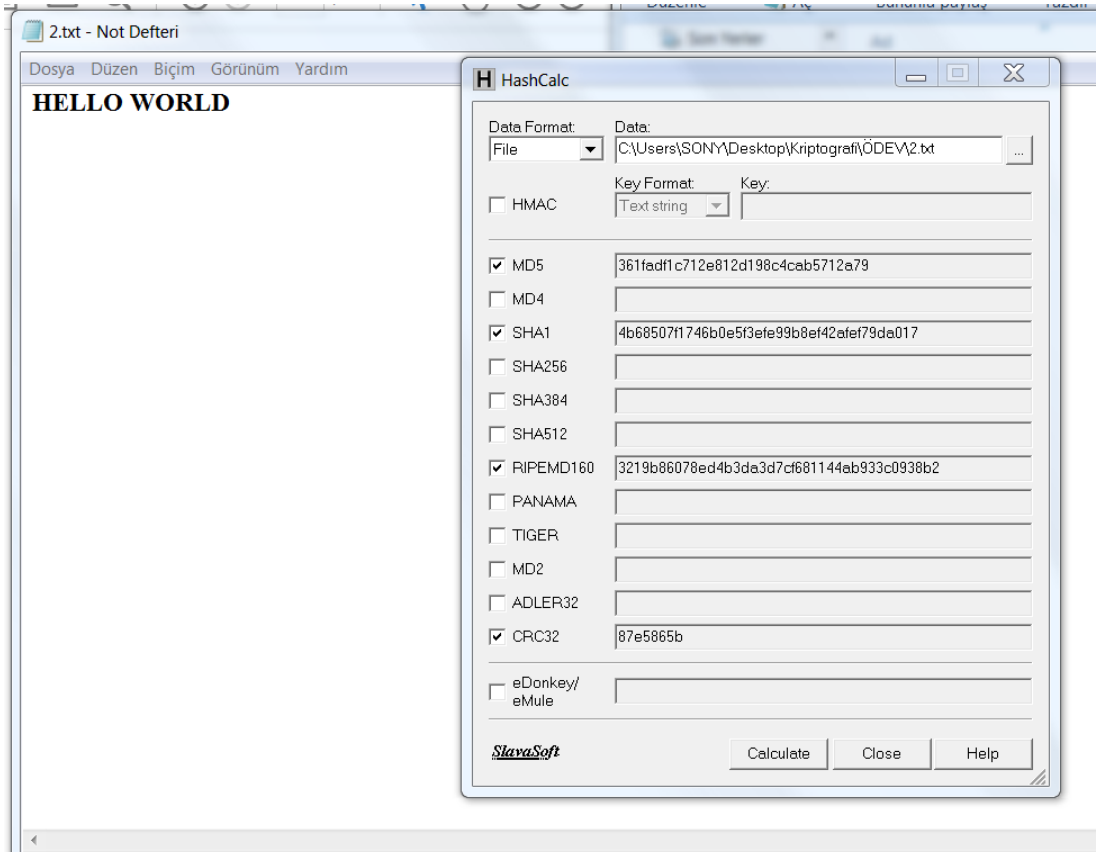
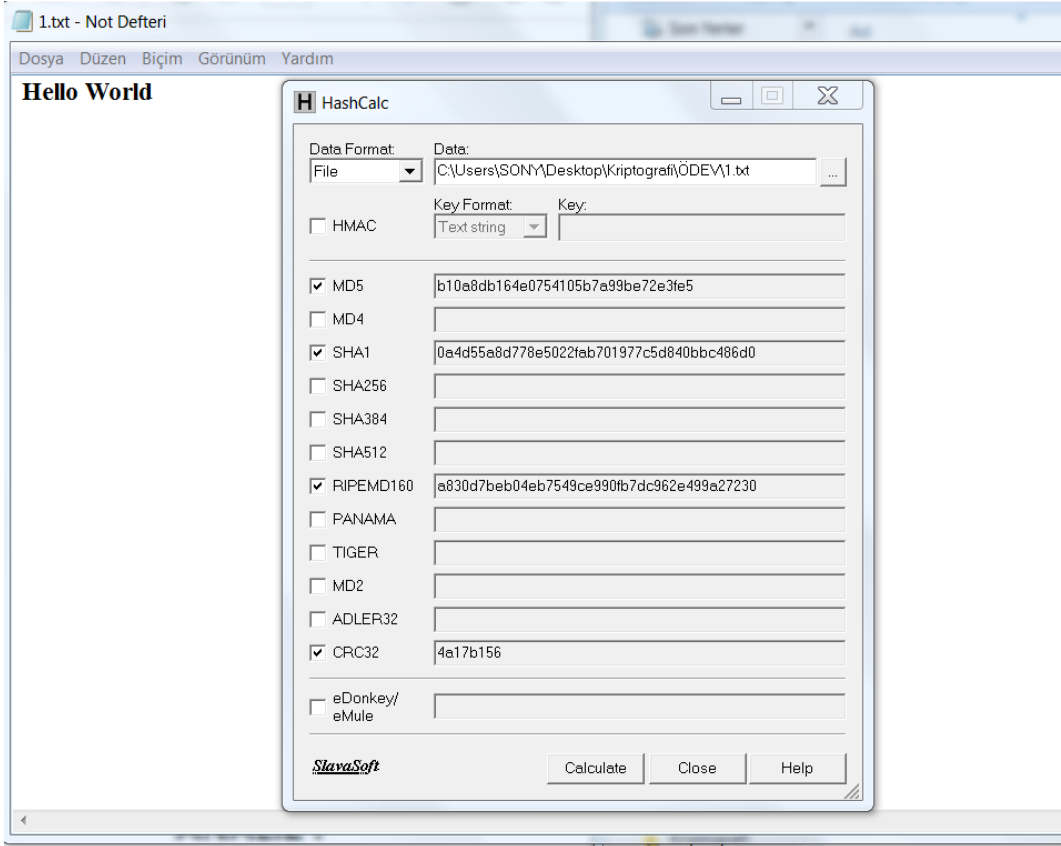
- Aynı özet değere sahip iki farklı doküman olabilir mi ?

$h: \{0,1\}^* \rightarrow \{0,1\}^n$

Hash fonksiyonu, herhangi bir uzunluktaki açık metni alıp sabit uzunlukta bir çıktı verir. Büyük bir tanım kümesinden sabit görüntü kümesine çoktan-bire eşlemedir.

h : Açık Metin \rightarrow Özet . Bu nedenle aynı özete sahip metinler bulunabilir.

*** Ödevde verilen Hello World ve HELLO WORLD ü denedim ve farklı md5 değerlerine sahip olduğunu gördüm.



Program Çıktım

```

betulgulcicek@ubuntu: ~/Desktop/BIL470_101044025_Betu_Gulcicek
betulgulcicek@ubuntu: ~/Desktop/BIL470_101044025_Betu_Gulcicek$ python BIL470_101044025_Betu_Gulcicek.py

MDS                                PATH

*****

0b0f28315663581De533bf626ca267b      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Fats-Domino-in-suit.jpg
fe7723e1f7b6c38321d236a949bb08b8    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/ec.jpg
b6d14b3ce2e2531d6e8142360f642e28    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Jon+Bon-Jovi+Friends+Benefit+Concert+Flk4IUCUcWl.jpg
35fe72d454c399f7c2e68563f14e2d      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Barry_White-gallery2.jpg
b3f2c4a5219a1487bfb7f6665f48a       /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/del-vikings.jpg
076cd0ff9a47a68328a4251f5f529737    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Bon-Jovi.jpg
719c3228d81917659b9adde2f0696bda    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/BoDiddle.jpg
d58ae6f4cde3258d811bbd939ebf7       /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Baris-Manco.jpg
8071c3ba5e2420abc2aa34a45c8ca0d     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Lewis-Jerry-Lee-1369933685.jpg
fa9e9145e23778f10ad2eef7f6e6138a    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/BonJovi_03.jpg
66882e16404dd61e43085d8ec99343b     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Barry-White-music-artist-pages.jpg
34ae788ad8db88112e4df1fe9292a51     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Big-Joe-Turner.jpg
13fe08a457e0e2f7b9293f32d604f4      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/JerryLeeLewis.jpg
2db1d7014e0809d9fafa02c257ab30      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/James-Brown.jpg
eb0dcccac83877639a9f4a720f0c6e42    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/San-Cooke.jpg
c23895e38a59f6c74ad09192d0f4d09     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Big-Joe-Turner-08.jpg
8815979c54463a9849ef3bf19b9d0      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/sancoke_1376575024559.jpg
027818bc672107eae4257595d732d3      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/James-Brown-007.jpg
70b7a37bb2ab79a9a6dc8415a3a3cf      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Baris-Manco2.jpg
df1920f17034482820f1fe4d3fe9fb2     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Rolling-Stones-the-rolling-stones-33506389-500-280.jpg
2420d149c15d6437b299d8112b5151a    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/SanCooke-celebrities-who-died-young-3731712-435-544.jpg
b0830a0bc7e113901bae40d6333e3d2c    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/SanCooke.jpg
c4f9e14c3c78cb088fae21ef7dbdbd      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Eddie-Cochran-rocknroll-remembered.jpg
d337a61859da7eb8b9a910e0bf552       /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/eddie-cochran.jpg
525dfc459933323fc3f38fa7e807db      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/san-cooke-zippo-kluv-getty-hulton-archiv.jpg
8651436121bd37f40ff5ab598332b1      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Baris-Manco.jpg
0c938c12f33308d2e0060554944435     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Samuel-Cook-A-K-A-San-Cooke-celebrities-who-died-young-3731712-435-544.jpg
63b2f7d9d4f0e4949d60b333c82cd      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Eddie-Cochran-Gallery_I.jpg
341d107d4cebd0a921f9a2ce91593d06    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Rolling-Stones.jpg
16f298a08af2d7f1d52d08bebf3f6c     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/hankwilliams.jpg
bfbb72616ab7ab4e3812a513c5c5c3     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/rolling-stone-617-489.jpg
da3deb171344d8d64d83b9e9634c91      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Jerry-Lee-Lewis.jpg
a80748dcdded1f0f1d02385eb5992       /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Bo-Diddle_8_M_36.jpg
e067234961aba3f959e7786f3766338     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Barry_White.jpg
39b05d41b5e371f49ac2c0b1baae2       /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/bo-diddle-7281970.jpg
0c6b01ecdfe05e4524834b0468cd4d      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/hank_williams.jpg
da3c23cab7b42704a666f4f22f3c2ba    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/del-vikings-sn.jpg
54ac4b205522bba8b0c4ae2b09b0bf6     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/del_vikings.jpg
8f4d44e4a8a9524c6d09a30b732a87       /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Big-Joe-Williams-1974-in-hamburg-a.jpg
9f33f2cccfca71f5b0cfff208c9a1f44     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/the-rolling-stones-4.jpg
0d52740743c382342d8859e2c88347      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Fats-Domino.jpg
76c63d69c5bd0c94f47a777fa72c9df    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/bigoeturner.jpg
21cfe5561f1d211298baf458f203a6a     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/delvikings18.jpg
e0973480fcdad2d00ff5f27af4f5d       /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Hank_Williams_Promotional_Photo.jpg
e0973480fcdad2d00ff5f27af4f5d       /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Hank_Williams_Promotional_Photo.jpg

betulgulcicek@ubuntu: ~/Desktop/BIL470_101044025_Betu_Gulcicek
d337a61859da7eb8b9a910e0bf552      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Eddie-Cochran-rocknroll-remembered.jpg
f251436121bd37f40ff5ab598332b1      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/eddie-cochran.jpg
8651436121bd37f40ff5ab598332b1      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/san-cooke-zippo-kluv-getty-hulton-archiv.jpg
0c938c12f33308d2e0060554944435     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Baris-Manco.jpg
63b2f7d9d4f0e4949d60b333c82cd      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Samuel-Cook-A-K-A-San-Cooke-celebrities-who-died-young-3731712-435-544.jpg
341d107d4cebd0a921f9a2ce91593d06    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Eddie-Cochran-Gallery_I.jpg
16f298a08af2d7f1d52d08bebf3f6c     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Rolling-Stones.jpg
bfbb72616ab7ab4e3812a513c5c5c3     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/hankwilliams.jpg
da3deb171344d8d64d83b9e9634c91      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/rolling-stone-617-489.jpg
a80748dcdded1f0f1d02385eb5992       /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Jerry-Lee-Lewis.jpg
e067234961aba3f959e7786f3766338     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Bo-Diddle_8_M_36.jpg
39b05d41b5e371f49ac2c0b1baae2       /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Barry_White.jpg
0c6b01ecdfe05e4524834b0468cd4d      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/bo-diddle-7281970.jpg
da3c23cab7b42704a666f4f22f3c2ba    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/hank_williams.jpg
54ac4b205522bba8b0c4ae2b09b0bf6     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/del-vikings-sn.jpg
8f4d44e4a8a9524c6d09a30b732a87       /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/del_vikings.jpg
9f33f2cccfca71f5b0cfff208c9a1f44     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Big-Joe-Williams-1974-in-hamburg-a.jpg
0d52740743c382342d8859e2c88347      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/the-rolling-stones-4.jpg
76c63d69c5bd0c94f47a777fa72c9df    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Fats-Domino.jpg
21cfe5561f1d211298baf458f203a6a     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/bigoeturner.jpg
e0973480fcdad2d00ff5f27af4f5d       /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/delvikings18.jpg
e0973480fcdad2d00ff5f27af4f5d       /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Hank_Williams_Promotional_Photo.jpg
e0973480fcdad2d00ff5f27af4f5d       /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Hank_Williams_Promotional_Photo.jpg
4f3b5cb0b4cee07c741b60976c3cc       /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/hank_williams.jpg
9934c77069b15452b0c4dc9a9e0a51e     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/delvikingsback.jpg
63b2f7d9d4f0e4949d60b333c82cd      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Bon_Jovi_001.jpg
7a3c1f118f87c7d66e9f9b478c77439     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Barry_White.jpg
3f0d4f1836d0015374274c96624c6e      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Fats-Domino-1.jpg
6d508b8f8b0d9a8c71bd07df937a5a     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/rolling-stones-72591463.jpg
500f3035ea38d1043e39842c0b970       /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Fats-Domino-Hamburg-1973-1605730021.jpg
b9d96a2a8a27b9f0f1a13b3ee9a886     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Baris-Manco.jpg
13bee90242f9b9a2e429f8a057145      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Barry-White-Staying-Power-Inlay.jpg
3a47b074b3c9d4f0092d6a42b98030      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Baris.jpg
fe084805cd5770def6f7216ac390dc      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/bo_diddle.jpg
e067234961aba3f959e7786f3766338     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/hank-williams1.jpg
508c24156f47ca2693b7d08b7f7c59eb    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/James-Brown-05.jpg
f33cfc7f3a329a5a43d5d1f7266da      /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Jerry-Lee-Lewis-1974-in-hamburg-a.jpg
742395d7142738a3c290304ac08f549     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/James-Brown-1963.jpg
65f0dc3a218d60f70f39b0ccf0b543     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/eddie-cochran.jpg
52216dc9a07433032f70957951f9d4f    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/bo-diddle.jpg
7b09c6b04ebdeae396a47f7f3727a71     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Big-Joe-Turner.jpg
44760b9a4856918495f2f79b9c9a1c91    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Jerry_Lee_Lewis.jpg
44760b9a4856918495f2f79b9c9a1c91    /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Bon_Jovi.jpg

*****

MDS Degeri Ayni Olan Resinler

e067234961aba3f959e7786f3766338     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/Barry_White.jpg
e067234961aba3f959e7786f3766338     /home/betulgulcicek/Desktop/BIL470_101044025_Betu_Gulcicek/Resinler/James-Brown-05.jpg

betulgulcicek@ubuntu: ~/Desktop/BIL470_101044025_Betu_Gulcicek$

```

Kaynak:

[1] "İleti Özümleme Algoritmaları", <http://www.belgeler.org/howto/md-algoritmalar.html>

BETÜL GÜLÇİÇEK

101044025